Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1713 03/27/15

~ Google Promises Glass! ~ People Are Talking! ~ Rogue Certs Warning!
~ Slack Hacked, Exposed! ~ India's IT Act Ruling! ~ Broken Age: Act 2!
~ Greatfire DDoS Attack! ~ More Atari "Re-births'? ~ Google Loses Ruling!

~ Who Gets Free Win 10? ~ Email Tracking Issues! ~ PS4 'Suspend/Resume'!

-* GOP Offers Net Neutrailty Deal *-
-* RadioShack To Sell Customer Data! *-
-* Wikipedia's Challenge to NSA Surveillance! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"

Last week, we thought that we saw the last of the white stuff, but the forecast calls for more snow to arrive over the weekend. I could have sworn that I surrendered a month ago! Enough already! I really don't mind that our current snowy terrain is dirty; we don't need a new coat of snow to clean it up!

Lots of interesting news this week, including some more tidbits pertaining to Atari's gaming heydays. Suer, we'd like to hear more about the computer side of Atari, but the gaming news always seems to pull the headlines. Anyway, I think you'll really enjoy them! Other "tech" stuff, there aee always interesting tidbits to look at, so you should be satisfied with those angles in case gaming isn't. Or, enjoy it all, I won't complain!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Broken Age: Act 2 Slated for April!
PS4 Getting 'Suspend/Resume' for Games!
'Bloodborne' Is Among The PS4's Best!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Broken Age: Act 2 Dated for April

Double Fine Productions has announced that Broken Age: Act 2 will be available on April 28th, the same day the full game will also debut on

PS4 and PS Vita.

Act 1 of the adventure game was released over a year ago on PC. The full Broken Age adventure is coming to PS4 and PS Vita through a partnership with the PlayStation Third Party Production team and it features cross buy and cross save.

Broken Age tells the story of Vella and Shay, a girl and boy from completely different worlds who seem to be leading strangely parallel lives. Vella has been chosen by her village to have the honor of being sacrificed to the terrible monster Mog Chothra, but having no interest in being devoured by a horrible beast, must go against ages old tradition and make her escape. Meanwhile somewhere in space, Shay is living a solitary life under the care of a very motherly computer, and whilst his every need is taken care of in every way imaginable, he wishes for nothing more than to break free from the monotonous safety of his daily life, and have some real adventures.

Funded by a record breaking crowdfunding campaign on Kickstarter, Broken Age features words, concept art and music from Tim Schafer, Peter Chan, and Peter McConnell, along with the unique art of Nathan Stapley.

PlayStation 4 Getting ’Suspend/Resume’ for Games at Long Last

Sony s PlayStation 4 will finally get a feature users first heard about at the console s unveiling in 2013.

Sony will push out a major PlayStation 4 update Thursday that will include the long-awaited suspend/resume feature, the company confirmed Wednesday. The update, PlayStation 4 v2.50, will be available for free, and include some other notable additions, including the ability to back up hard-drive data to a USB drive and then restore that back to the PlayStation 4.

But it s addition of the suspend/resume feature that might be the most important. Sony first announced the feature in 2013, promising that it would allow gamers to pause a game and put the console into rest mode. After booting the PlayStation 4 back up, gamers could pick up right where they left off without going through the main menu and choosing their game.

The addition of such a feature represents a major improvement. Historically, gamers would either need to save their progress and turn a console off or leave the console running if they had to leave and wanted to come back to a title. The suspend/resume feature eliminates those problems.

According to Sony, suspend/resume will work on nearly all of your PS4 games. The company didn t say which games would not work with the feature, but now that it ll be baked into the console, it s likely that most, if not all, of the games released on the PlayStation 4 would support it.

The update also includes a range of social features, including improved ways to find friends and play games with them. Sony has also added new accessibility options for players with disabilities, allowing them to customize button assignments, use text-to-speech features, and enlarge

text. PlayStation 4 owners will also be given the option to automatically install system software updates.

Sony s announcement comes just days after Microsoft previewed its own upcoming updates to its Xbox One console. Microsoft s updates will include improvements to party chats and the ability to see what the gamer did to earn an achievement.

Diabolically Difficult ’Bloodborne’ Is Among The PS4’s Best

Bloodborne is a game about hope.

It s also a game about death. It s about vile monsters smashing, slicing, clawing, and chewing you to bits. It s about horror, frustration, salty language, and broken controllers.

What keeps you playing Bloodborne, the incredibly challenging PS4-only role-playing game crafted by demented developer From Software, is a spark. It s hard to see, a flicker in the darkness often obscured by the rage of yet another failed attempt to kill a thing you are clearly in no shape to kill. But it s there, a glimmering beacon, a calm voice telling you that despite a learning curve shaped like a wall and hours spent futilely jabbing at creatures so hellish that you vaguely worry about the mental health of the people who created them, you are going to be OK.

You are going to win. And it s going to feel great.

Fans of From Software s infamous Souls series, which has rightfully earned a reputation as being among the most difficult of its generation, know the value of hope in the face of despair all too well. It s the secret sauce that s powered an impenetrably obtuse video game franchise to the heights of critical and commercial acclaim. It s also what makes Bloodborne one of the best PS4 games yet.

Anyone expecting that Bloodborne would be something of a departure from Demon s Souls and Dark Souls, perhaps a bit more inviting and less grinding in its difficulty, should prepare for the first of many disappointments. From its stressful gameplay loop to its online mechanics to the bright red YOU DIED message that mocks you roughly every 10 minutes, Bloodborne is Dark Souls 3 in all but name.

This time, you play a hunter wandering the once-pleasant city of Yharnam, now a gothic nightmare in the grip of an epidemic that s transformed its citizens into horrific creatures. Your task: kill the beasts and restore order. Crammed with confounding religious overtones and steeped in gore, the story isn t the star here. But a cohesive narrative isn t the point of these games, and it s all just absurd enough to keep you marching straight into Bloodborne s fiery video-game baptism.

At its core, Bloodborne plays like any of the past Souls games. You fight your way through monsters in an effort to locate an elusive progress-saving bonfire, though now it s a progress-saving lamp. Instead of acquiring souls by killing creatures, you acquire blood echoes, and when you die, you still have to race back to your corpse to retrieve them. Get killed on the way there and you lose your earnings forever. The Groundhog Day, love-it-or-hate-it Souls gameplay flow fight, die, run

back to your cash, forge ahead, die again, start the process anew is alive and well in Bloodborne.

But Bloodborne carves out its own identity. For example, monsters can now pick up your lost loot, requiring the additional step of killing whatever last killed you to get your cash back. Activating a lamp takes you back to a hub called the Hunter s Dream, a safe haven where you can buy and sell gear, repair and retrofit weapons, and boost your stats.

The biggest change, however, is found out in the field. Bloodborne is a faster, more aggressive game than Dark Souls II. Hiding behind a shield as a 20-foot-tall ogre tries to turn you into mush with a club the size of a Buick isn t an option because you really don t have any shields (I found one; it was useless). Magic is largely nonexistent, so you can t stand back and lob fireballs.

No, Bloodborne requires you to get up close and personal, dodging, back-stepping, staying just out of range of that Buick club as you dart in and out with your sword/axe/cleaver/hammer. It s a stiff challenge, requiring tight focus and a steady eye on your stamina meter, but it s also speedier and intrinsically more pleasing than standing back and firing arrows.

From Software also made a few concessions to keep you in the fight. You regain some health by immediately attacking the enemy who last injured you. You can also equip a gun as a secondary weapon, but don t expect to rip through Bloodborne with a bazooka. The guns serve mainly to stun tougher foes, opening them up for a big Visceral Attack that doles out huge damage. Good luck pulling it off regularly, though, because the only way to nail the timing is to figure it out on your own.

Part of the problem and this is obviously by design, so maybe it s not a problem so much as a fact is that Bloodborne doesn t believe in handholding tutorials. It walks you very quickly through its mechanics and doesn t care to re-explain itself. How does the Frenzy work? Where do I go to I equip these runes? What s the secret to stunning foes with guns? It s up to you to sort it all out.

While it s unclear in its systems, Bloodborne is sharply focused in its macabre sensibilities. The werewolves, zombies, giants, and giant werewolf zombies are meticulously built and thoroughly creepy, to a one. The game keeps upping the awful ante; after a few dozen hours, you ll duel snake-headed monstrosities, acid-spitting octo-things, and a numbers of creatures so gross and insane that despite decades spent ogling Dungeons & Dragons Monster Manuals, I couldn t describe them on a bet.

Invariably, Bloodborne s many roads lead to epic boss fights. You ll need to beat the bosses to open up new paths and acquire new abilities and true to form, the towering white wolf demon and electrically charged bear-skeleton thing are as wildly difficult as they look. But this is where Bloodborne really sinks its teeth into you.

If the multitude of regular monsters are weekly tests, Bloodborne s bosses are its final exams, and you need to study if you want to pass. The first time you fight a boss, you re going to die. But you ll learn a thing or two, and eventually you ll learn enough to know that despite the limited window to hit the beast in the foot, you can hit it in the foot. You just have to go do it.

That s the hope talking, and when it all comes together, it s intoxicating. After a couple of hours spent banging my head against the game s first tree-limbed behemoth of a boss, I dodged, leaped, parried, and stabbed it just enough times to kill it before it killed me. I took a victory lap around the house, arms raised. True, beyond Bloodborne s hills lie only bigger hills, but when you ve climbed one hill, you know you can climb more. You want to climb more.

Most of Bloodborne is spent this way: scouring its vast environments for hidden treasures and secret paths, stumbling upon something terrible, getting killed by it, and jogging back for a little revenge. It s repetitive, to be sure, and often the best way forward is to spend time farming the weaker bad guys for cash. You ll doubtlessly fling a controller across the room when you do something stupid and lose 45,000 blood echoes. But you re not mad at the game so much as at yourself. You should have been patient. You should have spent that cash when you had the chance. You should have been smarter. Fools rush into Bloodborne, and death rushes back out.

Fools also forget that Bloodborne has a multiplayer component. You can leave messages for fellow hunters (another holdover from the Souls games), and you can also invite players into your game to help take down bosses. It s still a little wonky you need to ring a bell, which costs yet another poorly explained currency called Insight, and then wait for someone to (maybe) come join you but it does work, and it can be immensely useful when you re out of ideas. If you also run out of things to kill (you), Bloodborne offers cool procedurally generated dungeons, which can also be played cooperatively. And for gamers looking to show off their skills, the game lets players invade each other s worlds and go mano a mano.

It s a big package, and Bloodborne occasionally buckles under its weight. The game looks great, all dark and gloomy and bloody and nasty, but the severe load times when you re respawning only serve to drive your failure home a few inches more. Occasional frame-rate issues can hamper fights against larger groups, a tall-enough order even when it s running smoothly.

Suffice it to say, Bloodborne isn t for everyone. It s unforgiving, repetitive, and bad for your blood pressure. But it s also mysterious, powerful, and good for your soul the best PS4 exclusive yet. What more could you have hoped for?

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Atari Might Reboot Tempest, Missile Command and Others

As its reboot of 1979 arcade title Asteroids hits Steam Early Access, publisher Atari says some of its other classic franchises might get the same treatment.

Tempest, Warlords, Adventure and Missile Command are among the titles that the firm is considering rebooting. In aid of this, the publisher is ’teaming up with young and innovative studios’.

This comes after the company blocked Tempest developer Jeff Minter from releasing his new shooter TxK on PS4, PC and Android. Atari believes TxK constitutes a copyright violation owing to its similarities with Tempest.

Earlier this year, Atari announced that it had decided to re-imagine Asteroids as open-world PC survival game Asteroids: Outpost.

This is part of our new strategy. We are going to be teaming up with young and innovative studios to take a refreshing look at each game from our extensive portfolio, said Atari COO Todd Shallbetter.

Releasing Asteroids: Outpost through the Early Access program will also help us get feedback from the community. Asteroids is the first of a long series of re-births, and we are considering doing the same for our other iconic games such as Warlords, Adventure, Tempest, Missile Command and many more.

Playing ’Space Invaders’ with Real Lasers Is Scary and Awesome

Thirty-seven years after its debut, it s still a lot of fun to watch the iconic Space Invaders aliens blink out of existence when your shot lands on screen.

But watching them catch fire? That s better. Way better.

Using a laser cutter, an Arduino mini-computer, and a terrific sense of imagination, a hobbyist in the U.K. has created a real-world version of the arcade classic that literally burns the aliens up when your aim is true.

"It s got aliens, lasers and general destruction so what s not to love, especially if you could replicate most of that functionality in the real world," said creator Martin Raynsford.

The project took about four months to conceptualize, but once Raynsford knew what he had to do, it took him just a few nights to put together, he says.

The bug-like creatures are made out of paper in this version, and when hit by the laser, they burst into satisfying flame. The shields are made of foam, and just like the game, they block the first shot by the player. That initial volley burns a hole through the shield, though, making subsequent blasts through it possible.

There s one big difference between this real-world version and the arcade game: the invaders don t shoot back, so it s basically a massacre. There is, however, a practical reason for that decision, as a reflecting laser could do some serious damage to the player s vision.

"I thought about mounting a rotating mirror behind the space invaders so they could shoot back but I decided I like my eyes a bit too much," says Raynsford.

Players play the game on a laptop, but what they re actually doing is controlling an 80-watt laser cutter that s firing beams at paper invaders clipped to metal plates. Those plates move left and right (and up and down) courtesy of stepper motors.

When you re playing with real lasers (and real fire), the consequences can be a lot more severe than a wasted quarter. So before launching the game, Raynsford conducted a test run (or, test burn, as he calls it). Good thing he did, as he learned the aliens were too tightly grouped, so hitting one would set off a chain reaction, burning down the entire row.

While fire can still spread in the current version, he says, it s much less likely now that he has reduced the size of the aliens.

The bad news? Raynsford isn t planning on manufacturing this thing, so unless you live near his workspace, odds are you re not going to get a chance to play it yourself. Until then, you re going to have to stick to more traditional electronic versions of the game.

How Atari Paved The Way for Mobile Gaming

The display of Atari hardware and software presented at the 2015 Game Developers Conference by the Videogame History Museum was a veritable treasure trove of video game majesty.

Before attendees at GDC entered an expo hall to play with experimental game controllers, and to try the games in the GDC Play exhibit, they had to pass by a temple dedicated to legendary video games. Display cases filled with Atari hardware, consoles and computers dating back to the beginning of the living room video game invasion of the late 1970s, were set up alongside working, legacy Atari consoles and games for GDC attendees to play.

"The younger developers probably aren’t too familiar with some of the stuff," John Hardie, one of the directors of the Videogame History Museum, told The Daily Dot. "Even the people who don’t quite know what it is, they seem to appreciate what it is, and they know that it’s valuable to preserve this history."

"It’s very rare to find industry people that don’t have some association with the history of the industry," Joseph Santulli, founder of the museum, told the Dot. "Every once in a while you get a young kid that will tell me Hey, this stuff came out all before I was even born,’ and you can give them a little bit of a primer as to what each thing is, but it’s pretty rare for somebody to not know."

"We’ve been collecting ourselves for over 30 years, my two partners and myself," Hardie said. "This weekend we’re picking up a Star Trek cockpit machine someone’s donating. Actually, it turns out to be signed by Leonard Nimoy."

Shortly before we spoke with Hardie and Santulli, they were given a copy of an Atari Panther developer kit by a GDC attendee. The Panther was developed by Atari at the same time the Jaguar console was in development. The Jaguar was released to the marketplace, whereas the Panther was not.

"We get people all the time coming up to us saying I have this, it’s sitting in my house, I’d much rather give it to you guys and have it on display,’" Hardie said. "A lot of the developers, the early game designers who we’ve befriended over the years... early Activision guys, early Atari guys, have donated their entire archives to us."

Nolan Bushnell, who founded Atari, Inc., has attended functions held by the museum. Among the items in the collection at GDC was a copy of a Puppy Pong machine, with Bushnell’s signature.

Part of the joy of attending these sorts of museum exhibitions is discovering hardware or peripherals that someone may have been completely unaware of, or had only read about but never seen in person. We had no idea the Atari Panther was a thing that existed, nor had we ever seen Puppy Pong.

We also had our first look at one of first coin-operated arcade games ever, Computer Space.

"It’s 1971, and these guys are developing the machine," Santulli said. "They didn’t have anything to work off of, other than How are we gonna get this game on a television set, and have people interact with it?’ That’s all they were working with. And it’s actually kind of amazing, although it doesn’t look anything like the cabinets later did."

"It’s got all of the other trimmings that you would expect," Santulli said. "A coin slot, controls in front of you, a television screen at approximately your eye level, and a score, to keep track of things. Despite the odd shape and look of it that didn’t catch on, they had most of the other ideas right."

While hardware like the Atari Panther and the Computer Space arcade machine may seem like mere historical curiosities, there are lessons relevant to the modern video game industry that developers like those at GDC can learn. From a certain point of view, old-school Atari games even have a leg up on modern games.

"There are some designers and developers now who are looking to what made games fun, and that was a big factor back when you only had 2k-4k [of memory] to work with," Hardie said. "The game had to focus on being fun, and not so much the graphics or whatever. And I think we’ve always said that, not everybody, but some of the modern games have lost that element. They have a lot of flashy graphics that look great, but are they really fun to play?"

According to Hardie, game designers will often stop at Videogame History Museum displays like those shown at E3, and look at old design documents, trying to figure out what made these old school games work, and why people loved them so much. The designers are looking for ideas on how to apply those lessons to game designs in the present day.

"I spent a lot of the day yesterday sitting down with developers in front of an Atari 2600, playing the game Outlaw," Santulli said. "What I did hear quite a bit from those developers was Oh, look, here’s some real simple gameplay elements that make the game, no matter how terrible it looks, that make the game fun I think they can definitely appreciate the fact that you’re working with such a limited amount of space and technology, but still able to make such a fun experience."

Hardie tends to stick with old-school games that only take 15 minutes or so to play, games like Space Invaders or Gyruss, and his tastes reflect the demographic that modern, mobile games have so deftly and lucratively played to. Hardie acknowledged that mobile games which focus on short play sessions are the spiritual inheritors of Atari's legacy.

"Modern games represent everything now, so [they] represent the complicated, Skyrim-type games [in which] you have an investment in time," Santulli said. "But, you could say that a lot of phone app games really do exactly what these games did back then. They're simple, they're meant for you to just sit down and play for a short amount of time, or they're not particularly built in a way where you have to worry about coming back to it again and again and again, with a password.

"There was a brief period of time before mobile apps became really popular," Santulli said. "I'm like Oh, these things are getting so complicated, let me go back and play my Atari because it's nice and simple.' But I think [video games] have gotten back to [simplicity]."

Santulli doesn't feel the influence of Atari games are limited to today's mobile games. He feels that Atari inspired a video game spirit that also lives on in some of the modern industry's biggest and highest-profile games, like Skyrim.

"In terms of how far can you go with a basic idea, and do it in a much bigger scale, my favorite game of all time was Adventure, on the Atari 2600, which is real simple," Santulli said. "You've got a little block, there's a sword, there's a couple dragons, and that's it. Get the chalice to the castle."

"To me, Skyrim is the ultimate Adventure. There are things going on that aren't on the screen that you're looking at. You have a weapon, you have bad guys, there's a quest that you have to complete. What lured me to [Adventure] when I was a kid, that simple quest, sometimes randomized, you didn't know exactly how it was going to play out, is basically what Skyrim is doing today, but of course with a studio of 300 people putting it all together."

The Videogame History Museum is planning on opening up a physical location, sometime between June and August. Having a location where voltages can be checked, and conditions can otherwise be controlled, is integral to making sure some of the hardware on display at GDC 2015 can be powered up for use without risking damage. Santulli thinks that even people who aren't involved in the video game industry, or who are enthusiasts, may have reason to visit.

"This is such an important part of culture, whether or not you're involved in it," Santulli said. "Whether or not you embrace it. You can't ignore it. If, for any reason at all, you needed to learn about it, or it came to you, you would be able to see, [the museum] fills in that block of why do people care about it, and we're really showing the entire lineage. How it started, why it was important, how it's actually developed our culture, how other pieces of culture have taken from video games and expanded upon themselves."

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Having Lost on Net Neutrality, Republicans Offer a Deal

When the FCC delivered a clear victory to advocates for net neutrality by announcing that it would treat the Internet as a common carrier, congressional Republicans reacted furiously. Speaker John Boehner denounced "overzealous government bureaucrats" for developing "a secret plan to put the federal government in control of the Internet." Senator Marco Rubio said the move "threatened to over-regulate the Internet." Other GOP lawmakers questioned whether President Obama had interfered with an independent regulator, since he had put out a statement endorsing net neutrality just a few months earlier. (At the time, Senator Ted Cruz compared the proposal to "Obamacare for the Internet.")

Yet nearly a month later, GOP lawmakers remain divided over how to respond; one proposal would explicitly block the agency’s change through a "resolution of disapproval," while another would actually cut the FCC’s budget and rein in some of its authority. Court challenges to the ruling are considered inevitable, and Republicans grilled FCC Chairman Tom Wheeler in a trio of hearings this week on Capitol Hill.

The most interesting possibility, however, is a bipartisan compromise that, according to its supporters, would legally bar the broadband industry from segmenting the Internet into "fast lanes" and "slow lanes" while also returning the web to its status as a communications service, not a common carrier, as it was for a dozen years before the FCC announced its change. While the difference may seem like a technicality, it has taken on great significance for activists concerned that powerful firms like AT&T, Verizon, or Comcast could block content based on their business interests, or favor one company over another by providing faster or slower loading speeds over its broadband network (streaming Netflix is a frequently-cited example of something that could be affected).

Proposing the new bill are some of the same senior Republicans Senator John Thune and Representatives Greg Walden and Fred Upton who long opposed the very concept of net neutrality but who have changed course as advocates for Internet freedom have gained momentum over the last year.

Wikipedia Challenge to NSA Surveillance Weighs Privacy Violation and Proper Targeting

What are the basics of Wikipedia s lawsuit against the National Security Agency? In a nutshell, the popular free-knowledge product believes the NSA surveillance of its foreign-based users is discouraging free speech for all people who use Wikipedia.

On March 10, 2015, the Wikimedia Foundation (the operator of Wikipedia), along with several human rights and media organizations, filed suit

called Wikimedia Foundation, et al. v. National Security Agency in the District Court of Maryland.
This lawsuit followed in the wake of the Edward Snowden leaks, and it alleges unconstitutional NSA surveillance practices. Specifically, Wikimedia and the plaintiffs say that known NSA surveillance of website users in other countries is discouraging online participation, and undermines their ability to carry out activities crucial to their missions.

Wikimedia and the remaining plaintiffs, represented by the American Civil Liberties Union, claim that the NSA s upstream surveillance practices violate free speech and privacy rights and exceed the agency s authority under the Foreign Intelligence Surveillance Act (or FISA).

Under Section 702 of the FISA Amendments Act of 2008 (FAA), the Attorney General and the Director of National Intelligence may authorize the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

Allegedly under the authority of the FAA, the NSA has been using upstream surveillance of communications of foreign and domestic persons. This type of surveillance involves seizing and searching internet communications (including emails, webpages, and instant messages) as they travel across the internet backbone of cables, switches, and routers. These text-based communications are then reviewed for any references to NSA search terms relating to a foreign NSA target.

The communications seized under this practice are those of foreign and U.S. persons. The NSA does not need individualized suspicion, but rather it can seize any communication to then determine if it references a specific target.

Wikipedia depends on U.S. and international readers and contributors to keep its website going, and believes that the anonymity of users allows people to freely express their ideas on controversial topics. In an op-ed published in the New York Times on March 10, Jimmy Wales, Founder of Wikipedia, and Lila Tretikov, Executive Director of the Wikimedia Foundation, stated that, [t]hese activities [viewing and editing Wikipedia articles] are sensitive and private: They can reveal everything from a person s political and religious beliefs to sexual orientation and medical conditions.

Wikimedia claims that the NSA s unconstitutional surveillance practices chill free speech by discouraging users in countries with repressive governments to contribute for fear of identification and retribution. According to Wales and Tretikov, [privacy] empowers us to read, write and communicate in confidence, without fear of persecution. Knowledge flourishes where privacy is protected.

The ACLU, Wikimedia, and the remaining plaintiffs are a few amongst several organizations that have challenged the constitutionality of NSA surveillance programs exposed in the aftermath of the Snowden leaks.

Slack Hacked, Leaving 500,000 User Emails Exposed

Slack Technologies, maker of a popular work-chat tool, had its user

database hacked in February.

Slack Technologies sure is making headlines. The San Francisco maker of an online workplace collaboration tool - which has drawn attention over its $2.76 billion market valuation - revealed a major hack of its user database Friday, releasing email addresses and potentially phone numbers of its 500,000 users.

Slack reported that hackers infiltrated its central user database, which includes email addresses and anything else added to users profiles, such as phone numbers or Skype IDs. Passwords, however, are encrypted in the database.

The hack reportedly took place over four days in February. Slack did not notify all users until publishing a blog post Friday morning and later emailing all users.

 The announcement was made as soon as we were able to confirm details, the post read.

The company reported that it detected suspicious activity in some accounts and notified those specific users earlier, a Slack spokesperson wrote to International Business Times in an email.

With the announcement of the hack, Slack pushed two new security features. Slack now supports two-factor authentication, a tool that requires users to confirm their log-in through two systems, such as with receiving a text message verification code. The security feature is something that many companies, including Apple with iMessage and Google with Gmail, have started to roll out and push to prevent privacy invasions.

"This further highlights the need for all organizations - both startups and established companies - to invest in post-infection software that can quickly identify security breaches and prevent valuable data theft," Paul Martini, CEO of cybersecurity provider iBoss, said in a statement.

Slack was developing two-factor authentication and was about a week away from releasing it, Reeve wrote, but the company chose an early launch after confirming the hack. Another new feature, "password kill switch," will allow administrators to terminate all user sessions and reset all passwords.

This isn t the first time Slack has been criticized for privacy and security concerns. In October 2014, the company gained media attention for leaving the names given to chat rooms visible to anyone. That flaw left potential secret departments and product development at companies, from the likes of Apple, Google and Facebook, exposed. Slack denied the design flaw as a bug but later clarified its policy.

Google Issues Warning on Rogue Chinese Digital TLS Certs

On Friday Google spotted unauthorized digital certificates for many of its domains that had been issued from Egypt. While Google did not see any misuse of the impersonated encryption certs, the company said the possibility was real for attackers to use them to intercept and monitor online traffic, according to a blog post on Monday.

According to the company, the bogus certificates, which are trusted by all major browsers and OSes, were issued by an Egypt-based intermediate cert authority named MCS Holdings, which operates under the China Internet Network Information Center (CNNIC) - a trusted nonprofit security certificate verification organization. CNNIC is also responsible for all Internet issues and is an extension of the Ministry of Information Industry for the Chinese government.

When Google contacted CNNIC about the bad certs, the company said that MCS only issued certificates for domains registered by the Chinese Internet center. However, researchers at Google did not find this to be the case.

"However, rather than keep the private key in a suitable HSM, MCS installed it in a man-in-the-middle proxy," wrote Adam Langley, security engineer for Google. "These devices intercept secure connections by masquerading as the intended destination and are sometimes used by companies to intercept their employees' secure traffic for monitoring or legal reasons. The employees' computers normally have to be configured to trust a proxy for it to be able to do this. However, in this case, the presumed proxy was given the full authority of a public CA [certificate authority], which is a serious breach of the CA system."

Along with alerting other tech vendors, including Microsoft and Apple, to the potentially dangerous certs, Google said that its Chrome Web browser running on any other platform would have automatically rejected the certificates thanks to the browser's built-in public key pinning security feature.

Mozilla also issued a statement saying that the next version of its Firefox browser (Firefox 37) will automatically revoke the certs issued by CNNIC and may conduct a security audit to confirm that "the CA updated their procedures, and using name constraints to constrain the CA's hierarchy to certain domains."

Microsoft has yet to comment on any actions it may be planning to take to block the rogue certs in Internet Explorer or Windows. According to the company's modern.IE developer site, a similar public key pinning feature found in Chrome is currently being considered for future versions of Internet Explorer.

Greatfire.org Faces Daily $30,000 Bill from DDoS Attack

An activist group that monitors Chinese web blocks has suffered a sustained distributed denial of service (DDoS) attack that has seen its server costs soar to $30,000 a day.

Censorship watchdog GreatFire.org's mission is to bring an end to Chinese censorship of the web, something it helps accomplish by mirroring sites, such as Google and Facebook, that are otherwise blocked by the Great Firewall of China.

By hosting the mirrors on content distribution networks (CDNs) that use the same hosting services that many legitimate Chinese sites rely on, such as Amazon Web Services, the group's strategy has worked up until now as the only effective response from the authorities would most likely also take out Chinese businesses.

In fact the strategy has been so successful that GreatFire previously told Google that it could help the company take down all Chinese censorship within 10 days.

Now, however, the group has experienced its first ever denial of service attack, receiving 2500 times more traffic than normal, prompting Greatfire admin and co-founder Charlie Smith to say:

This kind of attack is aggressive and is an exhibition of censorship by brute force. Attackers resort to tactics like this when they are left with no other options.

Smith said the attack, which is delivering up to 2.6 billion requests per hour, started on Thursday, shortly after an article about how the group used cloud services to circumvent censorship appeared on the Wall Street Journal website.

The magnitude of the attack poses a challenge to GreatFire and Smith admitted the group was unable to cope with the technical challenges.

Furthermore, the financial implications of the vast number of requests being made could cripple the group - it is currently unaware of how Amazon will react to the huge bandwidth bill currently being racked up:

Because of the number of requests we are receiving, our bandwidth costs have shot up to US$30,000 per day. Amazon, which is the service we are using, has not yet confirmed whether they will forgo this.

It’s not currently clear who may be behind the attack but people are looking to China as a suspect.

Not only do the authorities wish to block access to the sites GreatFire makes available, the country has been suspected of using similar tactics before to take down activist websites, and accusations of state-sponsored hacking are commonplace.

GreatFire says it doesn’t know who is behind the attack, but said "the attack coincides with increased pressure on our organization over the last few months".

Section 66A of IT Act Is Unconstitutional, Supreme Court Rules

The Supreme Court of India today struck down Section 66A of the Information Technology Act - a controversial law that allowed law enforcement officials to arrest people for posting "offensive" comments on social networks and other internet sites.

After hearing a clutch of petitions by defenders of free speech, the Supreme Court described the 2009 amendment to India’s Information Technology Act known as section 66A as vague and ambiguous and beyond ambit of the constitutional right to freedom of speech.

"Section 66A is unconstitutional and we have no hesitation in striking it down," said Justice R F Nariman, reading out the judgement. "The public’s right to know is directly affected by section 66A."

The Information Technology Act 2000 was amended in the year 2008 and this amended act contains the 66A section. Under this section, "Any person who sends, by means of a computer resource or a communication device, any information that is grossly offensive or has menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine."

But, the legality of section 66A has been in Question from years. The Supreme Court earlier had said that terms like ’illegal’, ’grossly offensive’ and ’menacing character’ were vague expressions and were likely to be dangerously twisted and misused.

Section 66A act stops people to share and express their different or controversial opinion freely that may not necessarily be dangerous or a subject of ’grossly offensive’ and ’menacing character’. Like for example, Theory of Evolution may be a false information for those religious people who believes that God created the whole world, but it may be useful information for those who study Science.

In 2012, two young women Shaheen Dhanda and Rinu Shrinivasan were arrested in Palghar in Thane district, Mumbai under the Section 66A act for posting comments against the shutdown in Mumbai following Shiv Sena leader Bal Thackeray’s death.

The charges on two young ladies were later quashed by a Mumbai court, but this first case filled under Section 66A followed a number of arrests across the country for uploading political cartoons or posting comments on social network, which sparked outrage and fierce debate about online censorship in India.

Some other controversial arrests under Section 66A of the IT act are as follows:
Recently, a class XII student was arrested for posting about Uttar Pradesh Minister Azam Khan on his Facebook timeline.

Businessman Ravi Srinivasan was booked by police for allegedly tweeting that the son of then union minister P Chidambaram, Karti Chidambaram, was ’corrupt’.

Last year, Devu Chodankar was arrested in Goa for writing on Goa+, a popular Facebook forum with over 47,000 members, that if elected to power, Modi would unleash a ’holocaust’.

Ambikesh Mahapatra, a Jadavpur University professor, was arrested in Kolkata for forwarding a cartoon about Mamata Banerjee.

The government argued that the section 66A of the IT act was needed to protect the government data from hackers, to which the court was not at all impressed as this situation was already dealt with viruses and hacking for which Section 65 of the IT Act was relevant.

Tinder Hack Tricks Men into Unknowingly Flirting With Each Other

In yet another example of how very hackable Tinder is, a programmer rigged the app with bait profiles, identified men who "liked" the phony female photos, and set them up to fling lust-filled come-ons at each other.

Cue the hilarity and loss of reading comprehension.

Screenshots of the confused conversations that followed were provided to The Verge, which already maintains a chat room that’s dedicated to the curation of staffers’ Tinder misadventures - a "bleak landscape," Michael Zelenko writes.

Now, the publication has a new genre to add to its Tinder compilation: the baffled but ever-hopeful male Tinder user.

The prank was set up by a California-based computer engineer who created a program that identified two men who "liked" one of his bait profiles.

One of the profiles featured a photo of a vlogger named Boxxy and one used the photo of an acquaintance who had given her consent.

The program relayed the men’s messages - "some aggressive, others mundane, but all of them unabashedly flirtatious" - back and forth through the dummy profile.

The engineer - The Verge gave him the pseudonym of "Patrick" - used to be a Tinder user and in fact met his current girlfriend there.

He was inspired to create the prank program by listening to women friends complain about their incoming Tinder messages:

The original idea was to throw that back into the face of the people doing it to see how they would react.

First, he started to build a Twitter bot to tweet out every first message received by a female friend, but Tinder was more amenable to the prank, he said.

That’s because Tinder’s API is notoriously vulnerable to being exploited.

Not only has it been used to promote a movie, it’s also been abused to expose users’ locations and to auto-like all female profiles.

(For what it’s worth, that last one’s not just a homemade hack anymore. Indiscriminate "likers" now have an app for that.)

The creator of the dude-on-dude hack told The Verge that pwning Tinder is a snap:
As long as you have a Facebook authentication token, you can behave as a robot as if you were a person.

"Patrick" said he finds the ethics of the exploit to be ambiguous.

Although he developed code to scramble phone numbers and otherwise prevented real-world meetings from taking place, he says he can’t help but think that the men he pranked kind of deserved it, given how eager they were to meet their new "girl" friends and how blind they were to

obvious red flags:

They ignore all the signs, they ignore all the weird things. When someone is so quick to meet up without any detail or know anything about the person at all - maybe it s deserved.

That sounds a bit like like victim-blaming to me. Regardless of how lustfully clueless the men were, they were still unwitting victims of a prank.

But Patrick has a good point. The exploit is yet another example of how people - or bots, in this case - can hide behind a fabricated persona online.

That’s why we warn people against accepting friend requests from people they don’t know on Facebook, and it’s why we tell people to be cautious about meeting in person someone they’ve only met online.

People tend to think of women and children as being potential victims, but this advice applies to all.

RadioShack To Auction Off Customer Data, Violating Own Privacy Policy

Retail chain RadioShack is looking to cash in the information it holds on its customers as part of its bankruptcy sale.

According to Hilco Streambank, personal data including over 65 million customers’ names and physical addresses, as well as 13 million email addresses, has been made available to the highest bidder.

All this despite the fact that the company’s online privacy policy quite clearly states:

We will not sell or rent your personally identifiable information to anyone at any time. We will not use any personal information beyond what is necessary to assist us in delivering to you the services you have requested. We may send personally identifiable information about you to other organizations when: We have your consent to share the information (you will be provided the opportunity to opt-out if you desire).

According to the Washington Post, the auction for RadioShack’s assets has already been completed, with Standard General - a hedge fund and RadioShack’s largest shareholder - the winner.

But the deal is yet to be completed as a bankruptcy court will need to approve the deal and, even then, there may be more legal hurdles to overcome before RadioShack can hand over any customer data.

According to a case filed in Texas, state regulators have offered up some objections to the proposed transaction, saying the sale would breach the company’s online privacy policy as well as in-store promises not to sell personal identifying information (PII).

The court filing also notes that the sale of customer data is illegal under state laws, which prevent the selling of personal information in violation of a company’s own privacy policies, as covered by the Texas Deceptive Trade Practices Act.

Responding to the possibility that RadioShack may sell its customer data in direct conflict with its stated privacy policy, New York Attorney General Eric Schneiderman said in a statement:

When a company collects private customer data on the condition that it will not be resold, it is the company s responsibility to uphold their end of the bargain. My office will continue to monitor Radio Shack s bankruptcy sale and whether it includes auctioning off private customer data. We are committed to taking appropriate action to protect New York consumers.

But it’s not only the authorities that are concerned about the privacy implications of this case - AT&T wants RadioShack to destroy the data, fearing that the data may fall into the hands of its competitors and claiming that some of it was obtained through the sale of its mobile contracts and is thus not RadioShack’s property in the first place.

To further complicate matters, a previous case in Manhattan may have some bearing after authorities approved the auctioning off of personal data under some circumstances.

In 2011, the Federal Trade Commission (FTC) gave the green light to the $13.9 million sale of Borders’ intellectual property to Barnes & Noble, on condition that the same privacy policy applied, the buyer operated within the same line of business, and if the data was sold in conjunction with other assets.

With Standard General reportedly looking to keep some RadioShack stores open, it may try to argue that any use of customer data may fall into a similar situation.
So what can consumers do to protect their data?

While the RadioShack ship may have already sailed, consumers should be aware that there is no legal requirement to hand over any information to a company beyond that which is required to complete the transaction.

So, next time a business asks for additional information that is incidental to the transaction being carried out, you are well within your rights to say no.

Google Loses Ruling in Safari Tracking Case

Google’s Safari issue goes back to nine months in 2011 and 2012.

In a landmark ruling, the UK’s Court of Appeal has dismissed Google’s request to prevent British Web users from suing the company over tracking cookies and privacy violations.

The decision was announced Friday, according to the BBC.

The case revolves around Apple’s Safari browser, Google’s Safari workaround, and cookies - small text files installed on PCs that record data on surfing activity. In spite of default privacy settings and user preferences - including an opt-out of consent to be tracked by cookies - Google’s tracking cookies gathered information on Safari browser users for nine months in 2011 and 2012.

Google profits from DoubleClick tracking cookies by installing them on computing devices and leading users to tailored advertisements. The DoubleClick ID Cookie, when settled within a user's browser, tracks and gathers data about the user based on Web activity and searches.

This information can include surfing habits, ethnicity, sexual interests, religious and political beliefs, and potentially financial data.

Three British computer users brought the case to court, arguing that Google ignored consumer wishes to not have tracking cookies installed on their machines.

Google argued the point was moot because consumers suffered no financial hardship due to the practice. The UK's Court of Appeal disagreed. According to the court's judgment:

"These claims raise serious issues which merit a trial. They concern what is alleged to have been the secret and blanket tracking and collation of information, often of an extremely private nature [...] about and associated with the claimants' Internet use, and the subsequent use of that information for about nine months. The case relates to the anxiety and distress this intrusion upon autonomy has caused."

UK Web users who accessed the web through Apple devices, including Macs, iPhones and iPads during the nine-month period now have carte blanche to take the tech giant to court if they feel their privacy has been invaded.

According to the BBC, Google is "disappointed with the court's decision."

The Google Action Group, a not-for-profit group set up to manage the claims of consumers against Google, applauded the decision.

"This is a David and Goliath victory," one of the claimants, Marc Bradshaw, said in a statement from the Google Action Group. "The Court of Appeal has ensured Google cannot use its vast resources to evade English justice. Ordinary computer users like me will now have the right to hold this giant to account before the courts for its unacceptable, immoral and unjust actions."

Dan Tench, a partner at Olswang who represents the claimants, said Google will now be held accountable for its choices.

"This is an important decision that prevents Google from evading or trivialising these very serious intrusions into the privacy of British consumers," he said in the statement. "Google, a company that makes billions from advertising knowledge, claims that it was unaware that was secretly tracking Apple users for a period of nine months and had argued that no harm was done because the matter was trivial as consumers had not lost out financially. The Court of Appeal saw these arguments for what they are: a breach of consumers' civil rights and actionable before the English courts."

Google did not immediately return a request for comment.

Microsoft Clears Up Just Who Gets Free Windows 10

Microsoft really wants people to upgrade to Windows 10 when it comes out this summer. So much that Microsoft announced at an event in January that upgrading to Windows 10 would be free for a year.

But then what?

I had a chance to sit down with Aaron Woodman, senior director of product marketing at Microsoft, to get the skinny on the Free Windows 10 offer.

To recap what we ve known since the Jan. 21 Windows 10 announcement: Microsoft will provide an upgrade from Windows 7 or Windows 8 to Windows 10 for free, for a period of one year from the release of Windows 10. There are some important details to this deal that were revealed, and a few that weren t. In my talk with Woodman, I got what I think is the definitive take on who will have to pay for Windows 10 and when, and who will not.

The Windows 10 upgrade will be free and a one-step process for consumers using the current versions of Windows 7 (SP1) and Windows 8 (8.1). If you re using an older version (Windows 7 or Windows 8 proper), you ll have to upgrade to the current version first. Those upgrades are free, too, but Windows 10 won t upgrade Windows 7 or 8 until it s made current. That ll make the upgrade a two-step process for users on older versions.

From one year after Windows 10 is launched, sometime this summer, you will be able to upgrade from Windows 7 SP1 or Windows 8.1 for free. But only if you are a specific kind of user.

The free-upgrade offer is for consumers upgrading their own computers. It s not available to to users of enterprise licenses of Windows: If you want to upgrade the machine on your desk at your big corporate job, the free offer won t apply. Your IT department won t get a bunch of free upgrades to give out; they ll have to pay for them. Likewise, PC manufacturers won t get free licenses for Windows 10 to install on new, unsold computers. For these guys, and in general, in no way is Windows free, Woodman said.

Woodman clarified for me that if you upgrade your PC to Windows 10 with the free offer, you won t be socked with a payment demand after some arbitrary period. Windows 10 isn t freemium. It won t convert from a free upgrade to a paid or subscription-supported operating system. He told me, clearly, Once you re on Windows 10, you re on Windows 10, and there will be no additional charge.

There are some individuals who won t be eligible for the offer, but not many. He implied that even if you miss the one-year free-upgrade window, it ll still be free: Basically no consumers will pay for Windows 10, Woodman said. Almost everybody will get the operating system either on a new PC (where the PC manufacturer pays for it), through work (where the company pays for an upgrade), or through the free-upgrade offer.

There are, though, edge cases that add up to a small fraction of Windows users. If you want a fresh copy of Windows 10 to install on a home-built computer or on a virtual machine (like Parallels or VMware Fusion on a Mac), you might have to pay for the operating system. Woodman said, We never said Windows is free, but also, We haven t made the decision on whether it will be free for these users, nor what it will cost if it is not free.

Microsoft sees everyone using Windows as a customer, no matter how they got the operating system or what they paid for it (if anything). The more customers Microsoft has, the more potential buyers it has of its own apps (like Office) and the more people who will be using the Windows App store, from which Microsoft will take a percentage of all sales. Furthermore, keeping Windows users on a current, safe version of Windows means better security and privacy for everybody. Hacked computers can infect other computers. Breaches and hacks cost companies (like Microsoft) money and customers.

Around the world, many of Windows 1.5 billion users are using pirated or, in Microsoft s lingo, non-genuine licenses of Windows. Woodman said that many don t even know it. ??Microsoft s goal is to get all Windows customers to take advantage of the upgrade offer and to get them on the most current, most secure version of the operating system. There s a lot of value in the ecosystem, Woodman said. There are a lot of future paying customers. Those customers are valuable to Windows.

Microsoft hasn t answered all the Windows 10 pricing question. The company still doesn t know (or is not revealing) the Windows 10 pricing for those who do have to pay for it, nor is it providing the full details of the amnesty program for upgrading pirated copies of Windows. As my talk with Woodman was winding down, a communications rep made sure to tell me, The story will get more clear as we talk about our product roadmap. But the one thing that is clear, so far, is this: If you have a personal computer running Windows 7 or 8, you won t have to pay for Windows 10. Ever.

A Clever Way To Tell Which of Your Emails Are Being Tracked

While you ve likely never heard of companies like Yesware, Bananatag, and Streak, they almost certainly know a good deal about you. Specifically, they know when you ve opened an email sent by one of their clients, where you are, what sort of device you re on, and whether you ve clicked a link, all without your awareness or consent.

That sort of email tracking is more common than you might think. A Chrome extension called Ugly Mail shows you who s guilty of doing it to your inbox.

Sonny Tulyaganov, Ugly Mail s creator, says he was inspired to write the tiny script when a friend told him about Streak, an email-tracking service whose Chrome extension has upwards of 300,000 users. Tulyaganov was appalled.

 [Streak] allowed users track emails, see when, where and what device were used to view email, he recalled to WIRED. I tried it out and found it very disturbing, so decided to see who is actually tracking emails in my inbox. Once the idea for Ugly Mail was born, it only took a few hours to make it a reality.

The reason it was so easy to create is that the kind of tracking it monitors is itself a simple procedure. Marketers or anyone who s inspired to snoop simply insert a transparent 1×1 image into an email. When that email is opened, the image pings the server it originated from with information like the time, your location, and the device you re using. It s a read receipt on steroids that you never signed up for.

Pixel tracking is a long-established practice, and there s nothing remotely illegal or even particularly discouraged about it; Google even has a support page dedicated to guiding advertisers through the process. That doesn t make it any less unsettling to see just how closely your inbox activity is being monitored.

Using Ugly Mail is as simple as the service is effective. Once you ve installed it, the code identifies emails that include tracking pixels from any of the three services mentioned above. Those messages will appear in your inbox with an eye icon next to the subject heading, letting you know that once clicked, it will alert the sender. Tulyaganov also confirmed to WIRED that Ugly Mail also doesn t store, save, or transmit any data from your Gmail account or computer; everything takes place on the user s end.

Ugly Mail appears to work as advertised in our test, but it has its limitations. It s only built for Gmail (sorry Outlookers) and is only available for Chrome, although Tulyaganov says that Firefox and Safari versions are in the works. And while it s effective against Yesware, Bananatag, and Streak, those are just three pixel-tracking providers in a sea of sneaking marketers. Tulyaganov has indicated that Ugly Mail will continue to add more tracking services to its list, but it s not clear yet how long that might take. The onrush of users after receiving top billing on Product Hunt may help speed up the process.

If you d like take take the extra step of just blocking pixel tracking altogether, another Chrome extension called PixelBlock also referenced on Product Hunt automatically prevents all attempts, instead of Ugly Mail s more passive strategy of simply informing you that they re happening.

Pixel tracking isn t going away any time soon, and Ugly Mail is an imperfect way to prevent it. But it still offers a valuable glimpse at the marketing machinations we re all exposed to every day, whether we re aware of them or not.

Glassholes Rejoice! Google Promises Glass 2.0

If the recent shuttering of the current version of Google Glass has left a hole in your wearable heart, fear not. Google executive chairman Eric Schmidt has promised that the team is committed to developing the company’s flagship wearable, which is being built under the leadership of Nest CEO Tony Fadell.

Speaking with The Wall Street Journal, Schmidt said that Glass is "a big and very fundamental platform for Google." The chairman noted that developing Glass is a long-term project not unlike the company’s self-driving car initiative, and that the wearable is being re-imagined rather than completely scrapped.

In January Google halted sales of the original version of Glass, which sold for a steep $1,500. At the same time, the company announced that the new Glass program would be led by Fadell, who currently runs Google-owned smart home company Nest and previously worked on Apple’s iPod and iPhone.

The restructuring of Glass gives Google an opportunity to address consumers’ biggest gripes with the device, namely its appearance, high

price and somewhat limited functionality.

"To be able to reach a broader audience, [Google] is going to have to adapt their solution to those who already have eyewear," ABI Research analyst Jeff Orr told us. "It's one thing to have something that looks like safety glasses... it's another thing to [offer] something a consumer would want to wear and feel comfortable doing so.

Aesthetics aside, Orr noted that the next Google Glass would benefit from better visibility for drivers, as well as a battery life long enough to last all day. The wearable's limited battery life was a major gripe in our review, as we were only able to squeeze about 5 hours of use out of the device on a full charge.

While Google has plenty to address for its next pair of smartglasses, Orr commends the company for breaking new ground, and believes that Glass could thrive under Fadell's leadership.

"This is a group within Google that now has a history of very strong consumer facing products," said Orr. "Having a team that understands hardware, human machine interface and how people behave in their environment [could] make a positive iteration," he continued.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.